
CYBERSEC 2022 臺灣資安大會
NOW
CHANGE
數位轉型 資安升級
SEP. 20-22 臺北南港展覽二館

IEC 62443 工控資安測試精要

高傳凱 博士

資策會資安所 副主任
資安檢測鑑識實驗室 技術主管

高傅凱

資策會 資安所 產業資安發展中心副主任
TAICS TC Network and Security WG1 組長
資策會 資安檢測鑑識實驗室 技術主管

+886-0955216185
marskao@iii.org.tw

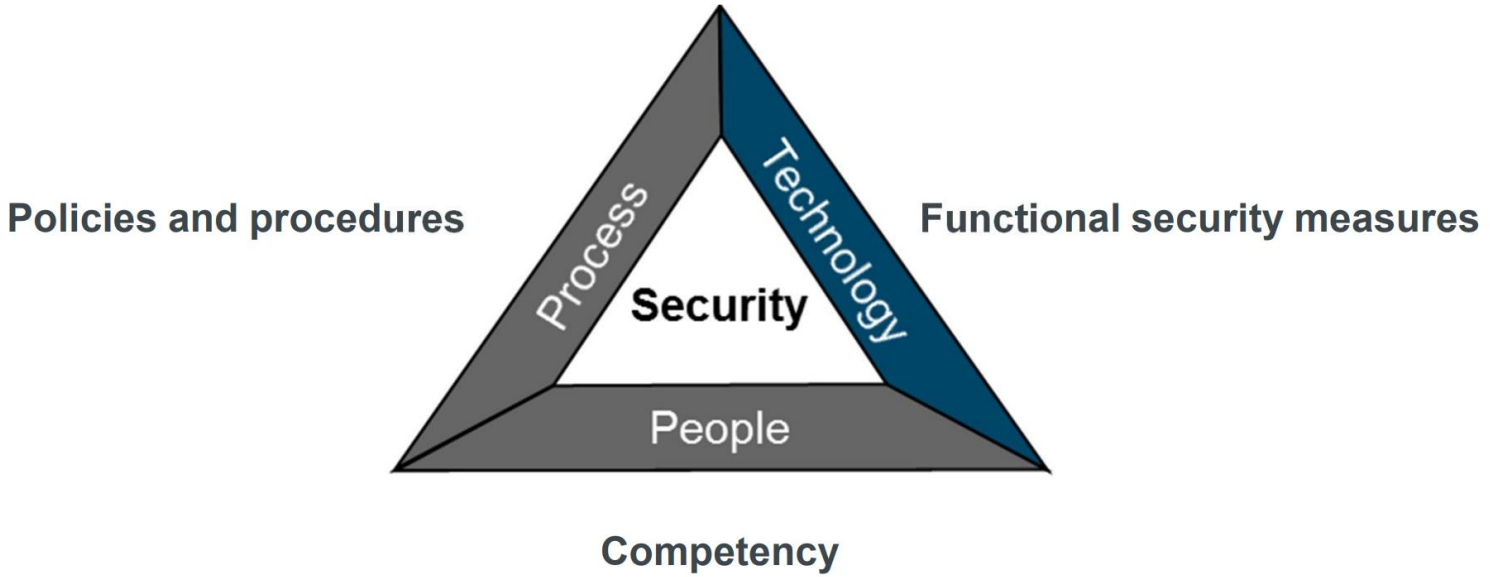
國立成功大學 電腦與通信工程研究所 博士

專長：物聯網設備資安檢測、資安標準研擬

願景：期待資安所成為資安研發的前導角色、政府資安政策的先鋒，帶動國家資安產業量能

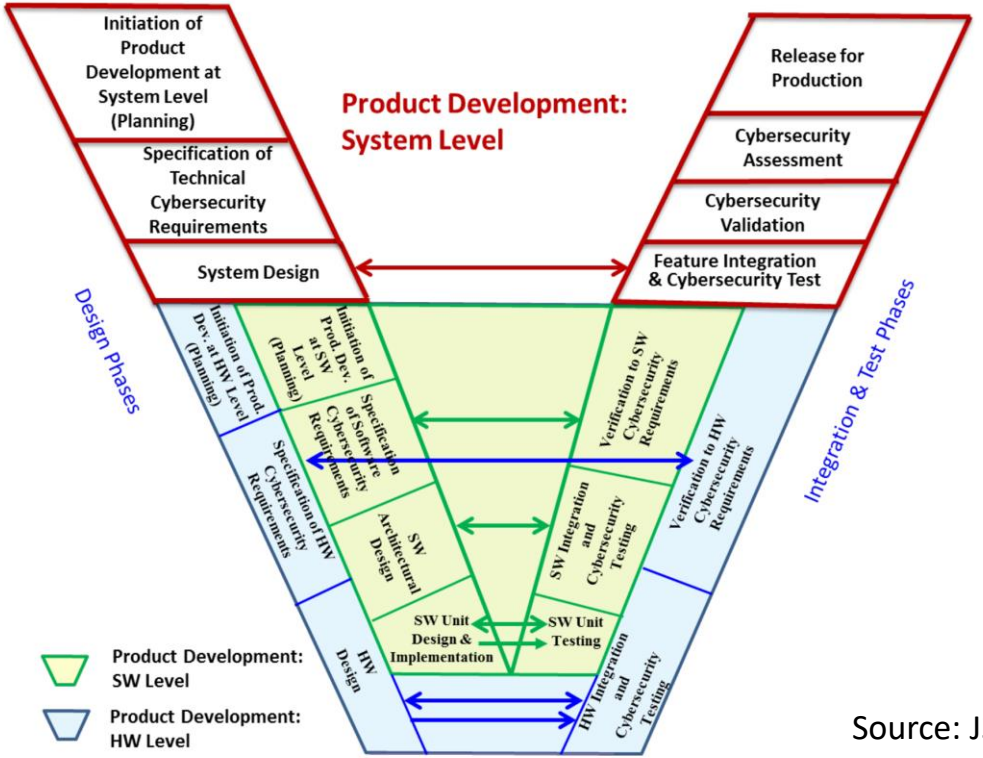
- **榮譽**
  - **2020 建構全國第一個資安國際交互認證體系(ISASecure)**
  - **2019 資策會資安所績優人員 技術菁英獎**
  - **2019 卓越計畫貢獻獎**
  - **2017~present 影像監控系列、智慧巴士系列、智慧路燈系列資安標準制定**
  - **2017 IEEE 論文審查委員**

資安是技術、程序、人



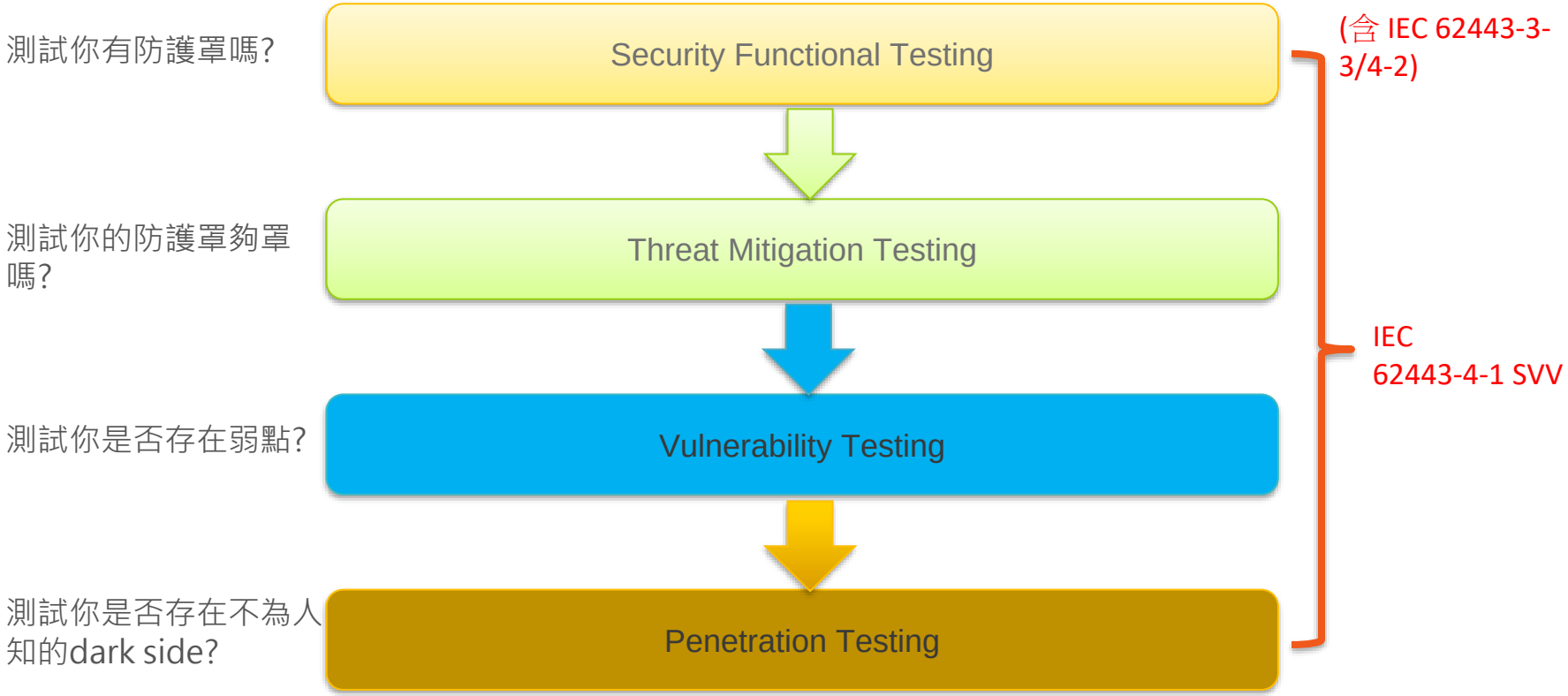
Source: Siemens

產品安全開發流程V model



Source: J3061

IEC 62443 縱深測試



Independence of SVV testers from developers

Test Type	Reference	Level of independence
Fundamental requirements testing	3-3, 4-2	Qualify Lab
Security requirements testing	SVV-1	Independent department
Threat mitigation testing	SVV-2	Independent department
Abuse case testing	SVV-3	Independent person
Static code analysis	SI-1	None
Attack surface analysis	SVV-3	Independent person
Known vulnerability scanning	SVV-3	Independent person
Software composition analysis	SVV-3	None
Penetration testing	SVV-4	Independent department

IEC 62443 - 3-3/4-2

- 標準合規測試
  - FR 1~FR 7
- 搭配全系統資安要求(3-3)配置合適的組件要件(4-2)
  - 例: CR 1.1認證功能是實做在Local?整合至System?
- 對開發團隊
  - 4-1安全開發紀錄(security context, design document, security guideline)、自我宣告、技術功能規格
- 對測試團隊
  - 測試SOP、測試環境、預檢測

SVV-1 Security Functional Testing

Security Function Requirement = $CSRS_{Risk}$ + FR_{4-2}

- **IEC 62443 part 3-3/4-2 安全功能基本要求(FR)**
  - 定義7個安全構面: IAC, UC, SI, DC, RDF, TRE, RA
  - 4種IACS組件: Software application, Embedded device, Host device, Network device
  - 4個安全等級: SL-C 1, SL-C 2, SL-C 3, SL-C 4

- **IEC 62443 part 3-2 風險評估產出之網絡安全要求規範 (CSRS)**
  - 4-2以外的安全功能
  - 例: 安全功能要求1:存取IACS功能之認證，須採用一次性憑證

備註: SVV-1還包括會影響可用性的常見穩定性測試，包括: Performance testing, Scalability testing, Boundary/edge condition testing, Stress testing, Malformed or unexpected input tests not specifically targeted at security

SVV-2 Threat Mitigation Testing

Mitigation Testing

Mitigation Thwarting Testing

SVV-3 Vulnerability Testing

- Abuse case / malformed / unexpected input testing

  透過模糊測試來進行

- Attack surface analysis

  測試驗證實際攻擊介面是否與風險評估一致，那實際上這些攻擊介面是否真存在資安洞，例：測試是否存在弱ACL, 未宣告port及網路服務弱點

- Black box known vulnerability scanning

  測試系統及網頁的資安弱點

- Binary executable file analysis
  - Known vulnerabilities, vulnerable libraries, security rule violations, compiler settings

  從二位元檔(執行檔)檢視所曝露出的資安弱點

- dynamic runtime resource management testing

  測試會不會因為handle釋放失敗、memory leak等情況而使得IACS發生DoS

SVV-4 Penetration testing

滲透測試框架

敏感性資料保護 確保帳號密碼、加解密金鑰等敏感性資料之儲存安全	資料安全	• 敏感性、隱私資料外洩 • 日誌外洩敏感性資料
應用程式安全 防止出廠預載應用程式及第三方函式庫不存在資安漏洞	應用程式安全	• Web (OWASP Top 10 2017) • App (行動應用App資安規範)
系統安全確保 保證作業系統、網路服務及韌體之安全性	系統安全	• 作業系統與網路服務安全 • 韌體解析、逆向工程、刷機 • 組態設定
存取控制 認證機制的落實、認證強度要求及用戶授權之管控	身分認證與授權	• web、SSH、App等認證缺陷 • 密碼破解
傳輸機密性 敏感資料的傳輸加密，及通訊協定所引發的資安威脅	通訊安全	• API授權缺陷、API Injection • 通訊協定漏洞(fuzzing) • 中間人攻擊、Air sniffing
實體安全確保 聚焦產品拆解、實體連接埠的管控及警示機制等	實體安全	• 韌體萃取 • 實體入侵(UART/JTEG)

參考 NIST SP 800-115, OWASP Top 10 IoT Vulnerability

Thank you